

Device Forensics Assignment 2



William Vasilev

20093711

Introduction

I am tasked with the investigation of an unknown device. I have been given a zip file that contains some evidence. I am supposed to examine the device and report on what I find about the device. I will be using iLEAPP to gather as much evidence as I could. This report will document the procedure I have taken and how I have obtained the evidence.

Investigate Strategy

My strategy is to use iLEAPP to find as much evidence as possible and try using DB browser to look through any database files.

iLEAPP is an IOS log parsing tool that was created by Alexis Brignoni. iLEAPP pulls digital evidence from a mobile device.

I will also be using a plist editor to check plist files.

Answers to Questions

1. Device Name

The device name is iPhone 8

I found the device name on iLEAPP under the case information section and in the Device details tab.

A screenshot of a computer

Description automatically generated

1. Software Version

The ios version of the device is 15.0.2.

I found the ios version in the same place I found the device name.

A screenshot of a computer

Description automatically generated

Found software version is Biome Sync report also.

File location: private\var\mobile\Library\Biome\sync\sync.db

A screenshot of a computer

Description automatically generated

Found full build version and build id.

Full build version: Version 15.0.2 (Build 19A404)

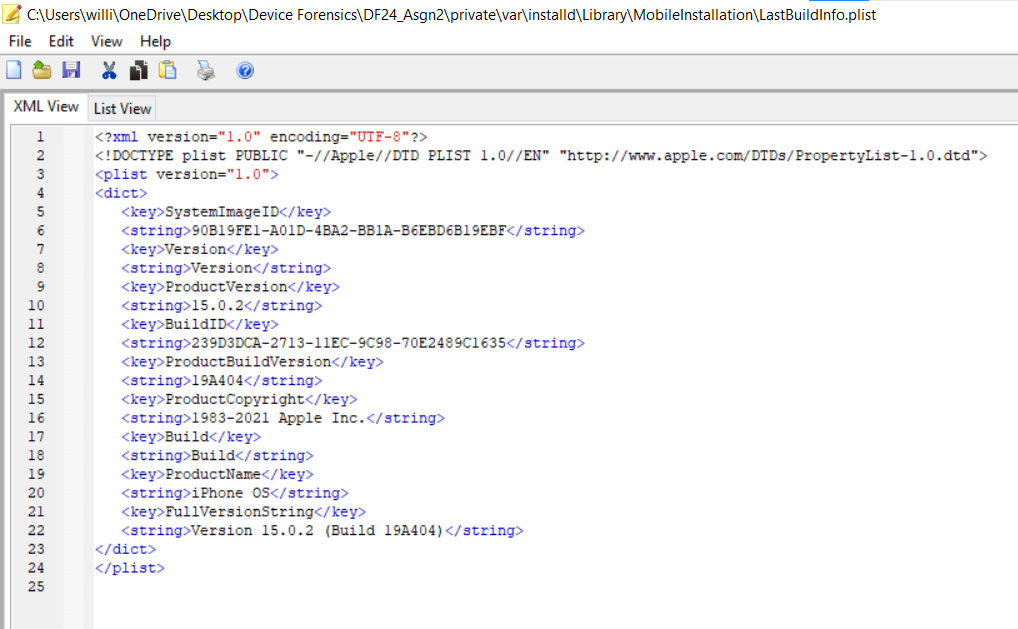
Build id: 239D3DCA-2713-11EC-9C98-70E2489C1635

File location: private\var\installd\Library\MobileInstallation\LastBuildInfo.plist

A screenshot of a computer

Description automatically generated

I also found the build version in a plist editor when I opened the file of the IOS build report.



1. Model

The model of the device is D20AP which is a iPhone 8.

I found the model in the same place as device name and software version.

A screenshot of a computer

Description automatically generated

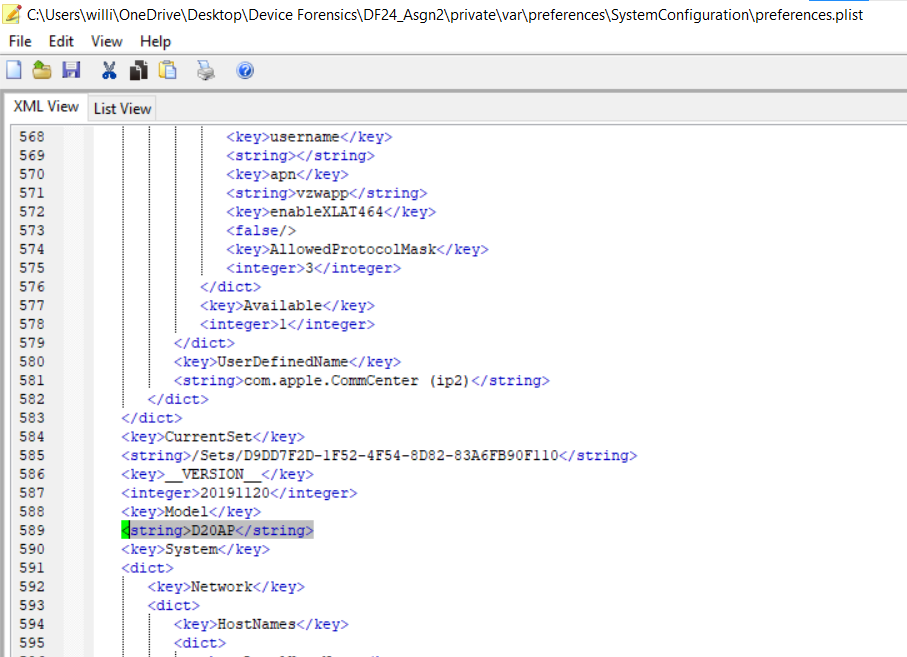
Found model in the device preferences report also.

File location: private\var\preferences\SystemConfiguration\preferences.plist

A screenshot of a computer

Description automatically generated

I also found the model in the plist report in a plist editor.



1. Serial Number

The serial number is nc.prod.pod2\_0831c498d2f04e9490e64b530fb9a5cf.

I found the serial number in the PK Passes report in section 2.

File location: private\var\mobile\Library\Passes\Cards\qB2Pg4J1rVjBRyE2ezPpfV1xob4=.pkpass\pass.json

A screenshot of a computer

Description automatically generated

I also found the serial number by opening the Json file it was in.



1. Wi-Fi Mac Address

The Wi-Fi MAC Address is: e0:eb:40:8f:46:2b

I found the Wi-Fi MAC address in the case information section.

A screenshot of a computer

Description automatically generated

Found WI-FI MAC address in the WIFI identifiers report too.

File location: private\var\preferences\SystemConfiguration\NetworkInterfaces.plist

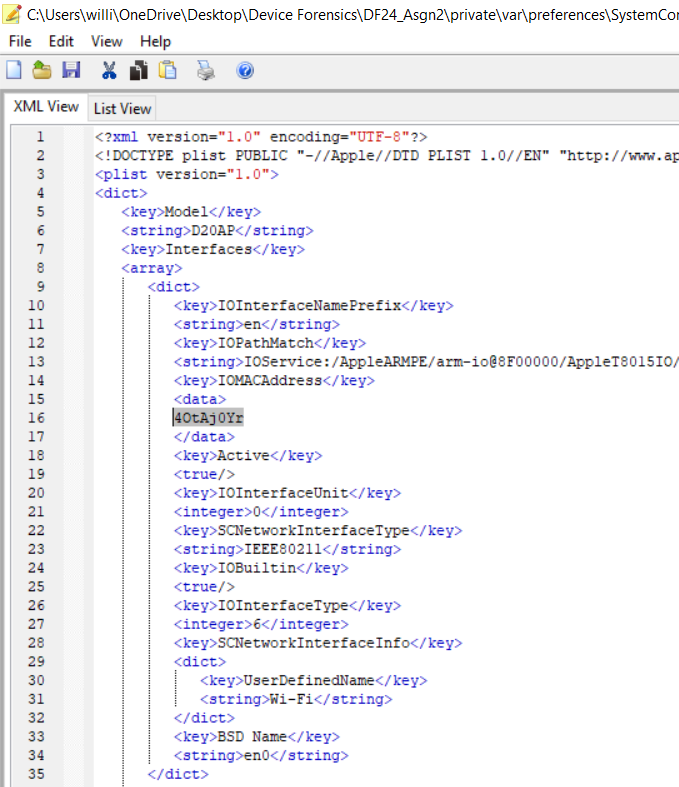
A screenshot of a computer

Description automatically generated

I also found the MAC Adress for Ethernet Adapter (en2), Ethernet Adapter (en1)

Which are e2:eb:40:8a:9d:6a and e2:eb:40:8a:9d:95.

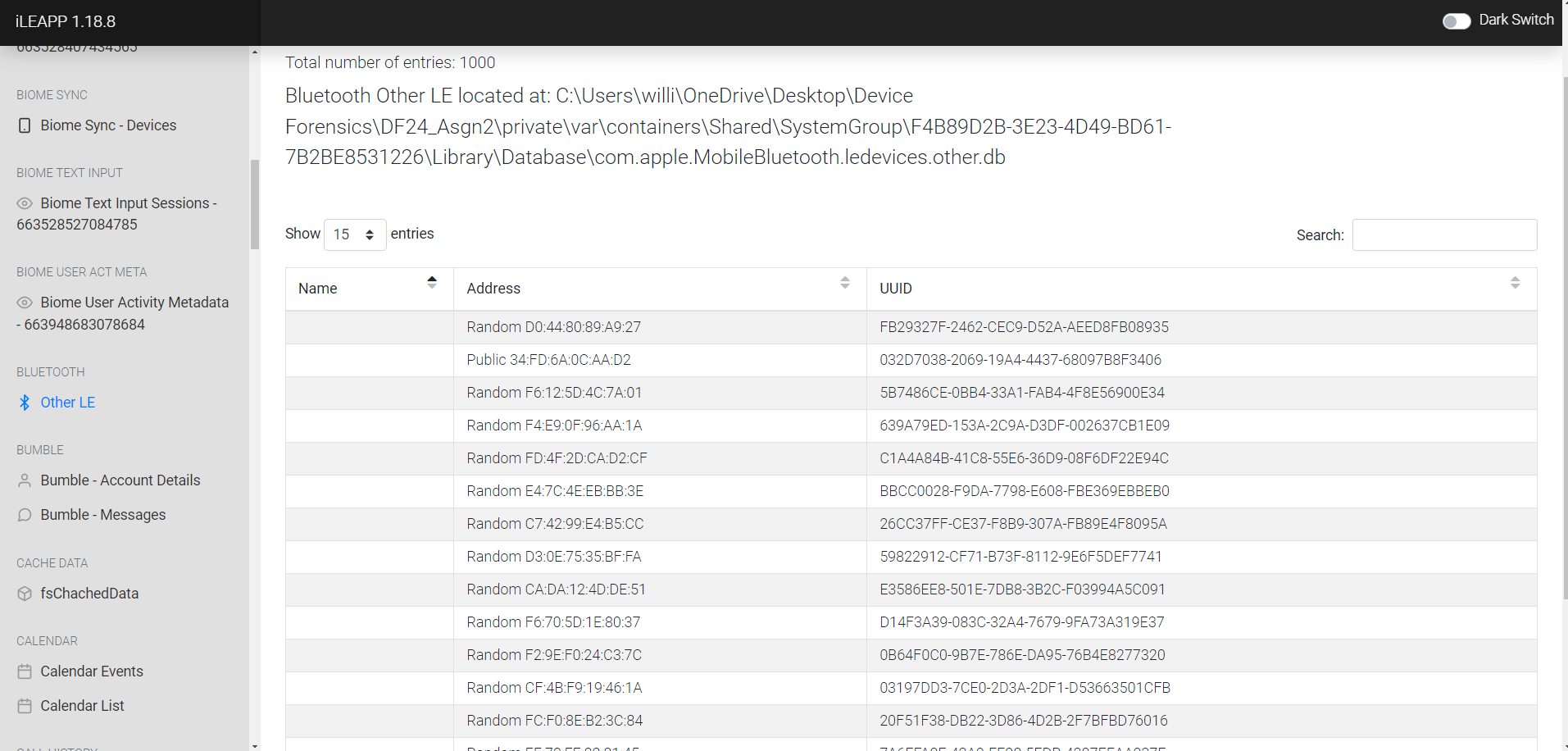
I also checked the plist file in a plist editor and when I saw the mac address it was different.



The mac address in the plist file shows 40tAj0Yr.

1. Bluetook Mac Address

The Bluetooth mac address is Public 34:FD:6A:0C:AA:D2.  
I found the blue tooth mac address In the other le section on iLEAPP.  
File location: \private\var\containers\Shared\SystemGroup\F4B89D2B-3E23-4D49-BD61-7B2BE8531226\Library\Database\com.apple.MobileBluetooth.ledevices.other.db



1. What was the last access point connected to

The last access point connected was b'ChamplainPSK'.

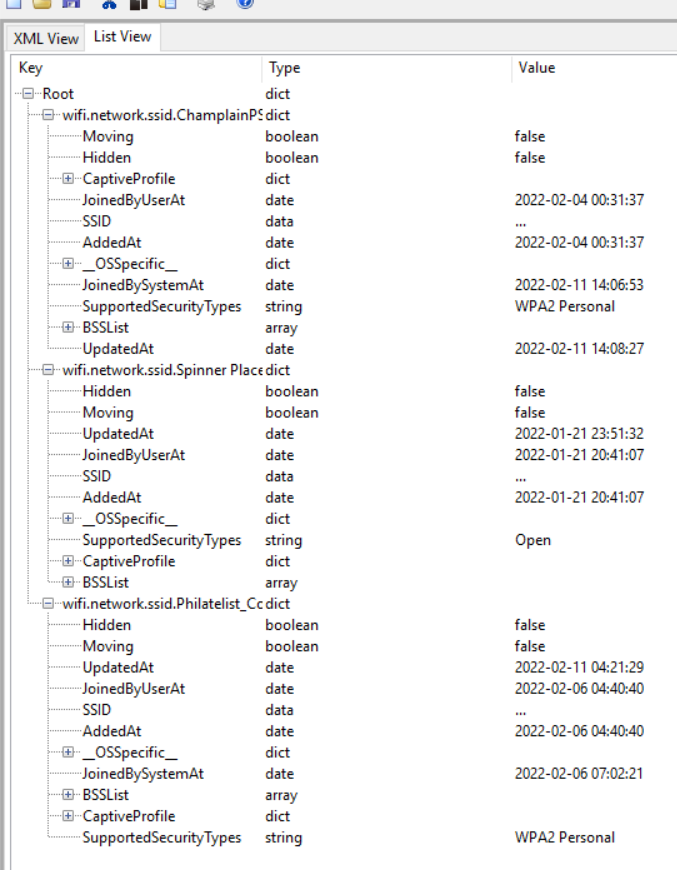
I found the last access point connected in the WI-FI known networks file based on last updated time.

File location: \private\var\mobile\Library\Logs\CrashReporter\DiagnosticLogs\sysdiagnose\IN\_PROGRESS\_sysdiagnose\_2022.02.14\_12-57-34-0500\_iPhone-OS\_iPhone\_19A404.tmp\WiFi\com.apple.wifi.known-networks.plist, \\?\C:\Users\willi\OneDrive\Desktop\Device Forensics\DF24\_Asgn2\private\var\preferences\com.apple.wifi.known-networks.plist

A screenshot of a computer

Description automatically generated

I also check the plist file in the plist editor.



1. Phone Number

The phone number is 19732941683.

I found the phone number in the case information page.

A screenshot of a phone number

Description automatically generated

I also found the phone number in the IMEI – IMSI Report.

File location: private\var\wireless\Library\Preferences\com.apple.commcenter.plist

A screenshot of a computer

Description automatically generated

I also found the phone number in the plist file.

A screenshot of a computer program

Description automatically generated

1. IMEI

The IMEI number if this device is 353219108442509.

I found the IMEI number in the case information.

A screenshot of a computer

Description automatically generated

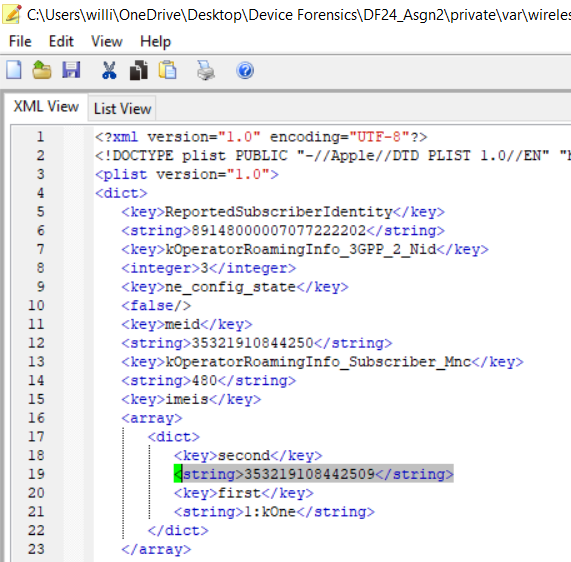
Found the IMEI in the device data report also.

File location: private\var\wireless\Library\Preferences\com.apple.commcenter.device\_specific\_nobackup.plist

A screenshot of a device data report

Description automatically generated

I also found the IMEI number in the plist file.



1. Data Partition size  
   The data partition size is 8.06 gb.

I found the partition size by going to the properties of the device folder.

A screenshot of a computer

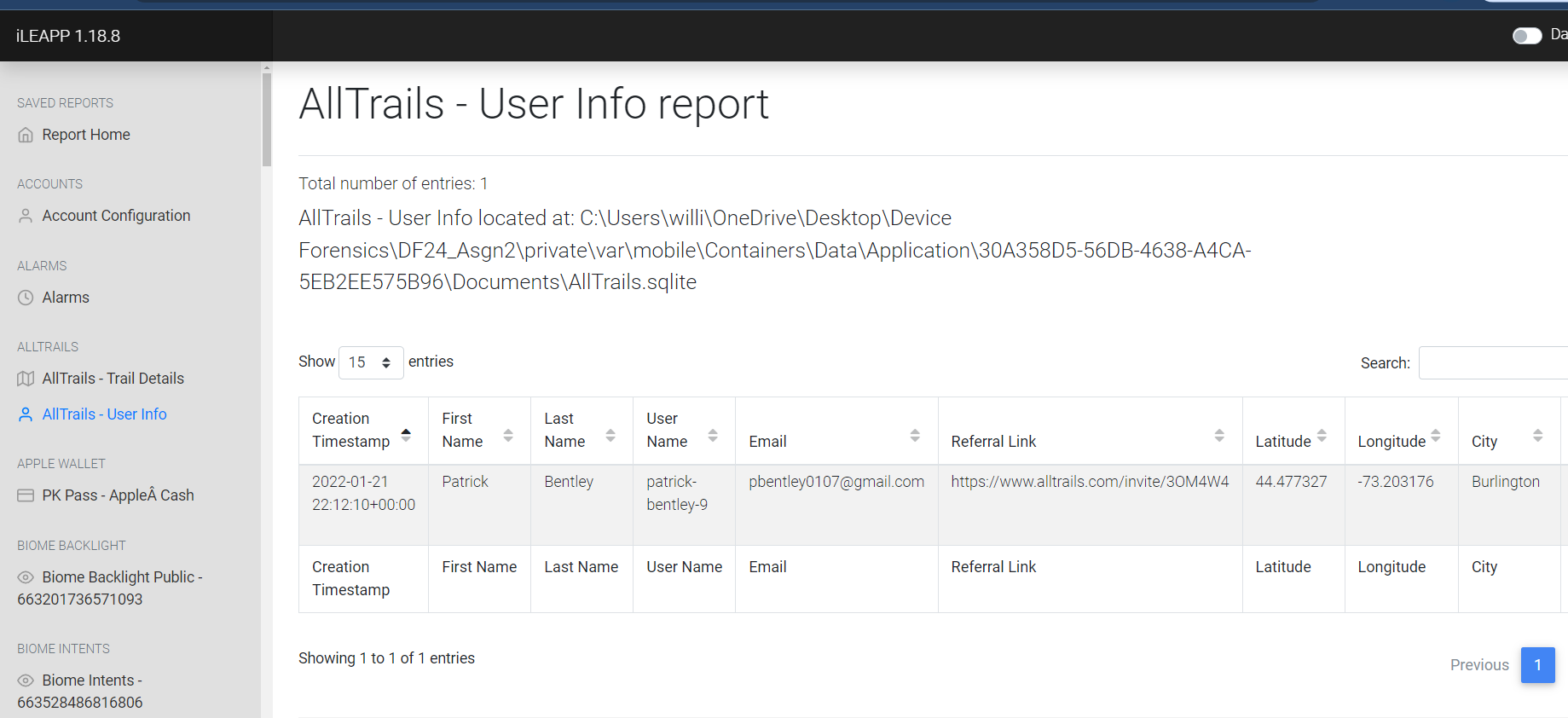
Description automatically generated

1. Owner name

The name of the owner is Patrick Bentley.

I found the name of the owner in multiple places, first being in the ALL Trails user info report.

File location: private\var\mobile\Containers\Data\Application\30A358D5-56DB-4638-A4CA-5EB2EE575B96\Documents\AllTrails.sqlite



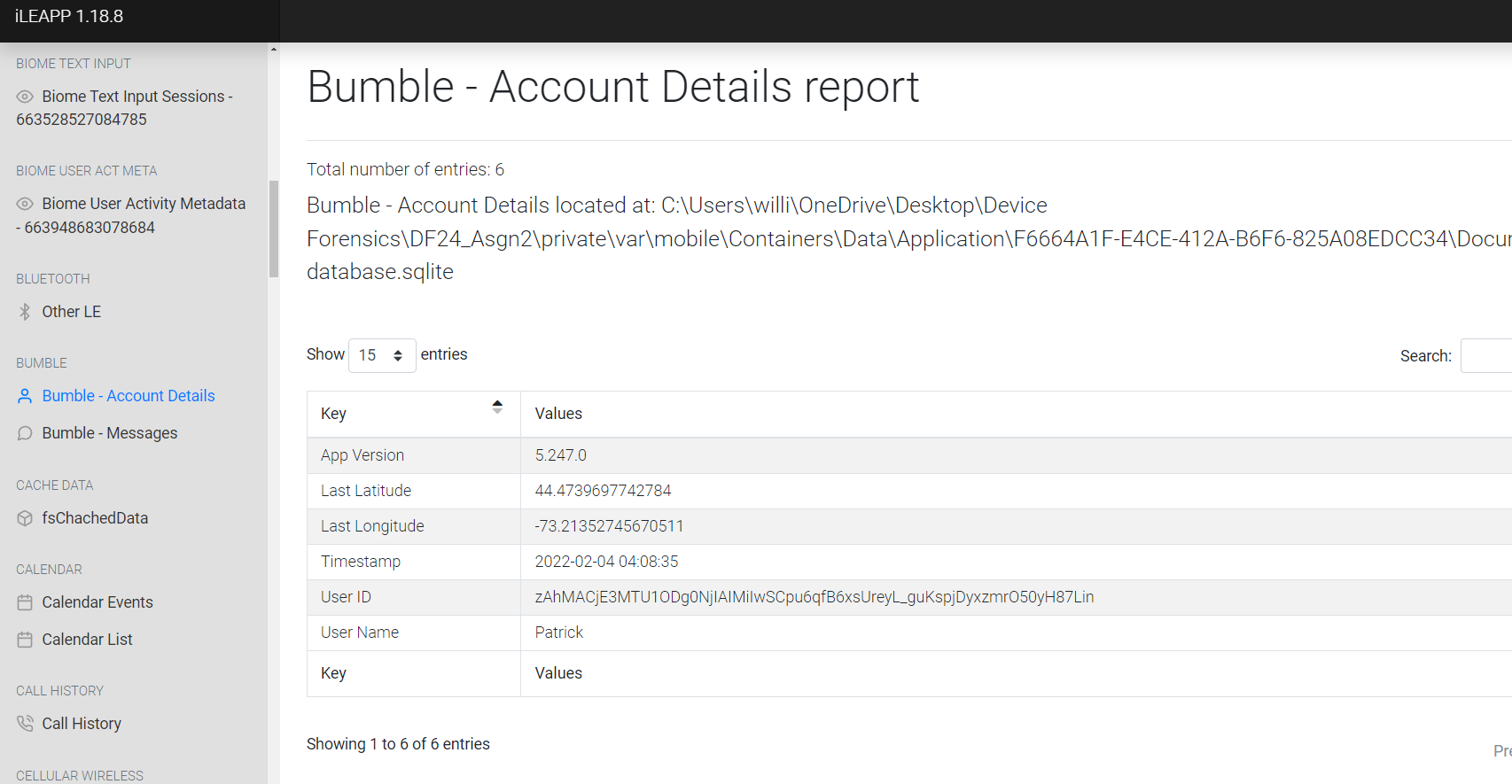
In biome intents I found a group id that shows Patrick.

File location: private\var\mobile\Library\Biome\streams\public\AppIntent\local\663528486816806



Also in Bumble account details report.

File location: private\var\mobile\Containers\Data\Application\F6664A1F-E4CE-412A-B6F6-825A08EDCC34\Documents\yap-database.sqlite



And in discord account report.

File location: private\var\mobile\Containers\Data\Application\80C6D157-4E08-4C34-8A6F-FA3F7D5EE229\Documents\mmkv\mmkv.default

A screenshot of a computer

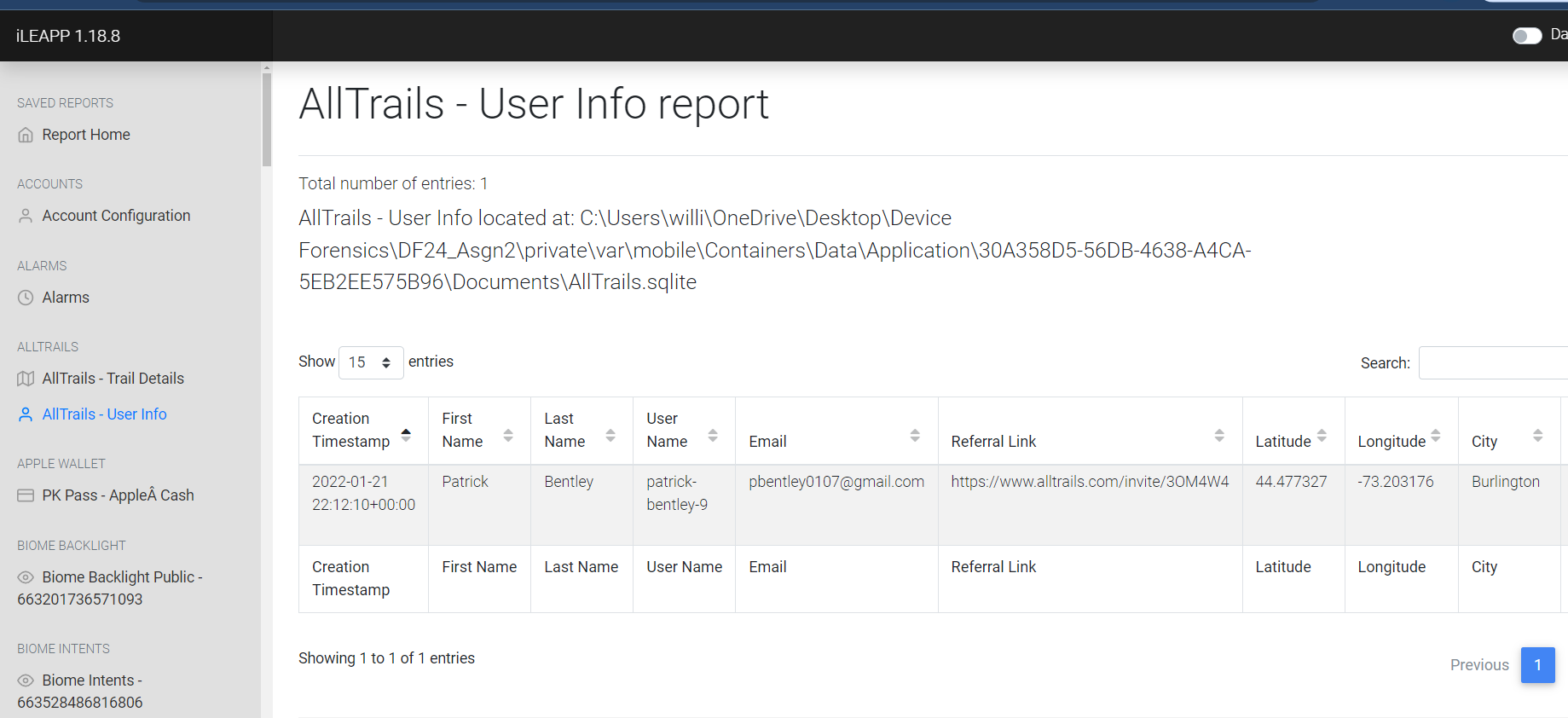
Description automatically generated

1. Email Account

The email account is [pbentley0107@gmail.com](mailto:pbentley0107@gmail.com).

I found the email account in All trails user report.

File location: private\var\mobile\Containers\Data\Application\30A358D5-56DB-4638-A4CA-5EB2EE575B96\Documents\AllTrails.sqlite



And in discord account report.

File location: private\var\mobile\Containers\Data\Application\80C6D157-4E08-4C34-8A6F-FA3F7D5EE229\Documents\mmkv\mmkv.default

A screenshot of a computer

Description automatically generated

1. Passcode (or unlock mechanism)

The unlock mechanism is fingerprint scanner.

I found the unlock mechanism in the IMEI – IMSI report.

File location: private\var\wireless\Library\Preferences\com.apple.commcenter.plist

A screenshot of a computer

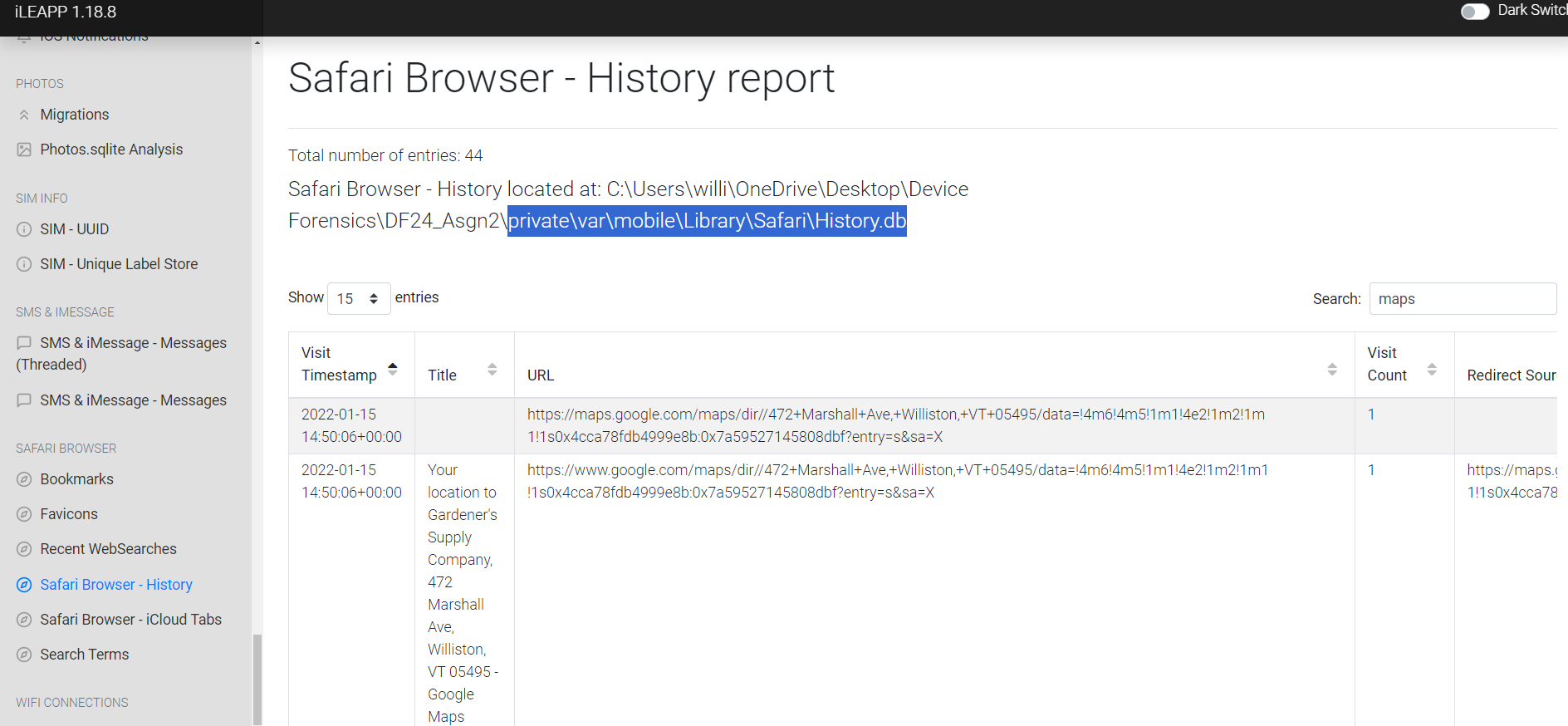
Description automatically generated

1. What Google maps url was visited using Safari?

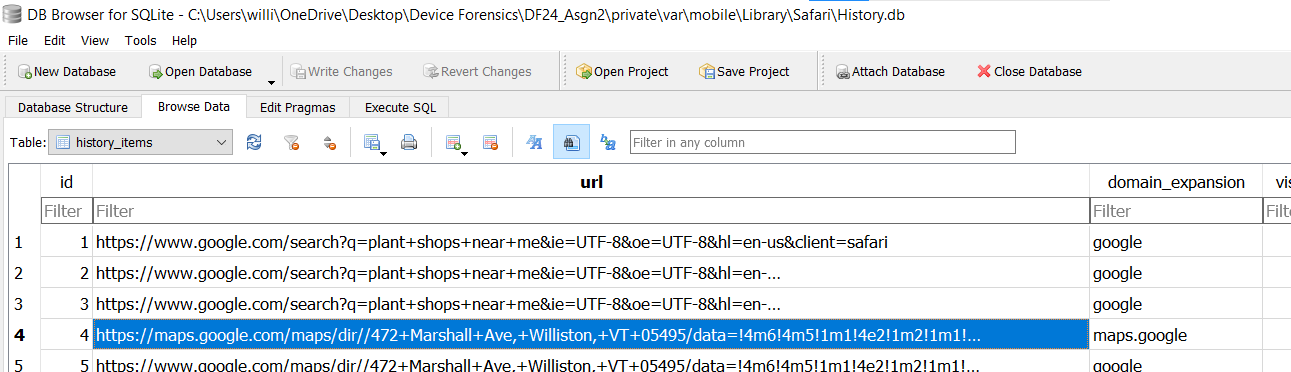
The google maps url that was visited using safari was [https://www.google.com/maps/dir//472+Marshall+Ave,+Williston,+VT+05495/data=!4m6!4m5!1m1!4e2!1m2!1m1 !1s0x4cca78fdb4999e8b:0x7a59527145808dbf?entry=s&sa=X](https://www.google.com/maps/dir//472+Marshall+Ave,+Williston,+VT+05495/data=!4m6!4m5!1m1!4e2!1m2!1m1%20!1s0x4cca78fdb4999e8b:0x7a59527145808dbf?entry=s&sa=X)

I found the location in safari history report.

File location: private\var\mobile\Library\Safari\History.db.

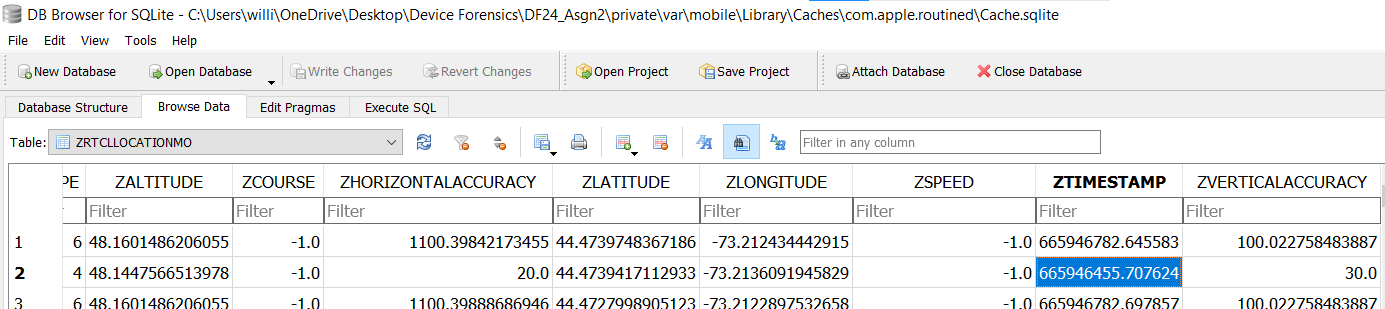


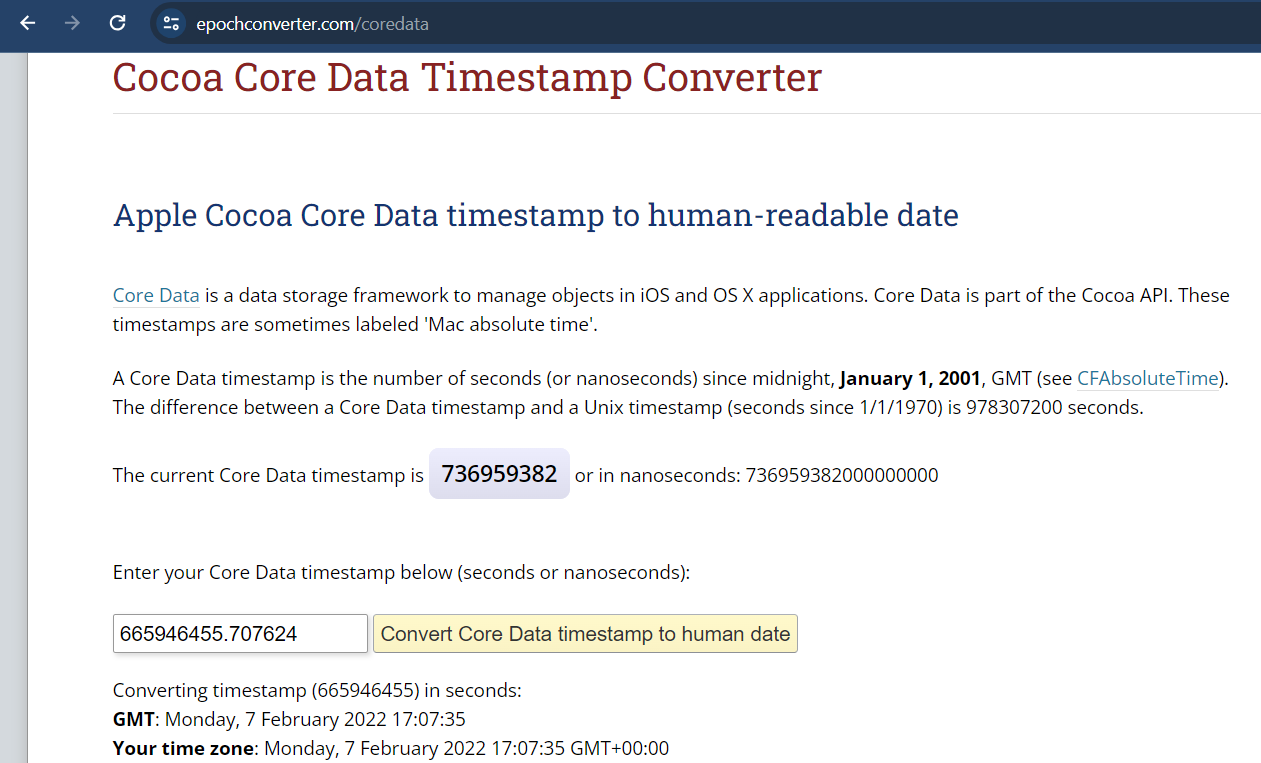
I also checked the history db of safari and the google maps url was the same.



1. Where was the device on Monday, February 7, 2022 5:07:35 PM? (should be formatted: XX.XXXXXXXX, -XX.XXXXXXXX)

The location of the device was 44.4739417112933, -73.2136091945829.  
I found this in the C:\Users\willi\OneDrive\Desktop\Device Forensics\DF24\_Asgn2\private\var\mobile\Library\Caches\com.apple.routined\Cache.sqlite database.



The timestamp of the database was in Apple Cocoa Core Data Timestamp. I had to convert the timestamp to readable human text, I did this using a timestamp converter online. <https://www.epochconverter.com/coredata> 

Once I converted the timestamp I saw the time was Monday, February 7, 2022 5:07:35 PM so the latitude and longitude of this time is where the device was.

1. How many times was Youtube visited on Safari?

Youtube was visited 2 times but there are other instances of YouTube which also have a visit count of 2.

I found this in the safari browser history report.

File location: private\var\mobile\Library\Safari\History.db

A screenshot of a computer

Description automatically generated

I also checked the history db and saw youtube with visit count 2.

A screenshot of a computer

Description automatically generated

1. When was the phone last rebooted? (YYYY-MM-DD HH:MM:SS)?

The phone was last rebooted on “2022-02-14 11:44:13”.

I found where the phone was last rebooted in the State – Reboots Report.

File location: private\var\installd\Library\Logs\MobileInstallation\mobile\_installation.log.1

A screenshot of a computer

Description automatically generated

1. What was the Microsoft Access code received by the user on Sunday, January 30, 2022 2:04:17.818 AM?

The Microsoft access code that was received was “1380”.

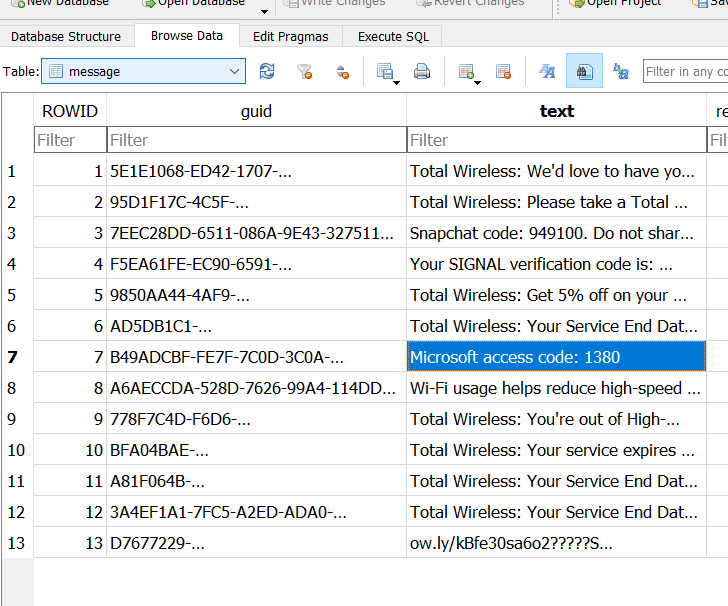
I found this in the SMS and imessage report.

File location: private\var\mobile\Library\SMS\sms.db

A screenshot of a computer

Description automatically generated

I also checked the sms db file and saw the same Microsoft code.



1. How many reviews did the user leave in the All Trails app?

I found 4 snapshots of trail app reviews, all reviews had the same rating and message and were all created at the same time. There is 1 review in total that the user has left on the trails app.

File location: private\var\mobile\Containers\Data\Application\30A358D5-56DB-4638-A4CA-5EB2EE575B96\Library\SplashBoard\Snapshots\sceneID\_com.alltrails.AllTrails-default\0ADA708C-8C44-4E32-AB7F-26A9D91EB100@2x.ktx

A screenshot of a computer

Description automatically generated

1. What is the hex code of the colour assigned to birthday events in the calendar app?

The birthday hex code is #8295AF.

I found the calander db file by navigating to the Calendar list report on iLEAPP.

File location: private\var\mobile\Library\Calendar\Calendar.sqlitedbA screenshot of a computer

Description automatically generated

I then navigated to the file and viewed the database in sqlite.

A screenshot of a computer

Description automatically generated

Conclusion

Overall, I am happy with the information I was able to retrieve, using iLEAPP was a huge help in finding information and sqlite db browser was useful to reassure me in knowing my answers were correct. I was unsure at first with how I was going to find the partition size because I thought I had to find the size within the files but instead I just used file explorer properties to find the size. The plist editor I used was also helpful to do my due diligence and gave me the confidence to know that my answers were correct.